

#5

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

1998年12月 7日

出 願 番 号  
Application Number:

平成10年特許願第347235号

出 願 人  
Applicant (s):

株式会社日立製作所

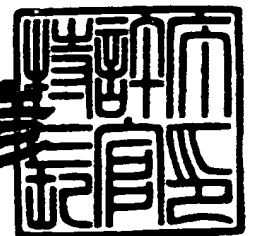
Serial No. 09/455,363  
Filed: 12/6/99  
Mattingly, Stanger & Malur, P.C.  
ASA. 838

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 1月14日

特許庁長官  
Commissioner,  
Patent Office

近 藤 隆 彦



出証番号 出証特平11-3093457

【書類名】 特許願

【整理番号】 K98054181

【提出日】 平成10年12月 7日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/28

【発明の名称】 通信ネットワークシステムの管理方法および情報中継装置

【請求項の数】 3

【発明者】

    【住所又は居所】 神奈川県海老名市下今泉 8 1 0 番地 株式会社日立製作所 サーバ開発本部内

    【氏名】 土屋 一暁

【発明者】

    【住所又は居所】 神奈川県海老名市下今泉 8 1 0 番地 株式会社日立製作所 サーバ開発本部内

    【氏名】 野崎 信司

【特許出願人】

    【識別番号】 000005108

    【氏名又は名称】 株式会社日立製作所

【代理人】

    【識別番号】 100080001

    【弁理士】

    【氏名又は名称】 筒井 大和

    【電話番号】 03-3366-0787

【手数料の表示】

    【予納台帳番号】 006909

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

【物件名】	図面	1
【物件名】	要約書	1
【プルーフの要否】	要	

【書類名】 明細書

【発明の名称】 通信ネットワークシステムの管理方法および情報中継装置

【特許請求の範囲】

【請求項 1】 ネットワーク端末またはネットワーク中継装置が接続される複数の入出力ポートと、個々の前記入出力ポートと前記ネットワーク端末またはネットワーク中継装置に付与されたネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方を対応付けて格納する制御テーブルと、前記制御テーブルに基づいて複数の前記入出力ポートの各々に接続された前記ネットワーク端末またはネットワーク中継装置の相互間での通信情報の授受を行うとともに、前記通信情報に含まれる前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と前記入出力ポートとの対応関係の変化を学習して前記制御テーブルを更新することで、前記入出力ポートに対する前記ネットワーク端末またはネットワーク中継装置の接続状態の動的な変更を可能にする中継処理手段とを含む情報中継装置を用いた通信ネットワークシステムの管理方法であって、

個々のネットワーク端末に対応した前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と、当該ネットワーク端末のユーザ名およびパスワードとが対応付けて格納された認証テーブルを設定する第 1 のステップと、

前記制御テーブルの更新を伴う前記通信情報の授受が発生した時、前記通信情報の授受および前記制御テーブルの更新に先立って、前記通信情報の送信元および送信先の少なくとも一方のユーザに対して、前記ユーザ名およびパスワードの入力を要求し、入力されたユーザ名およびパスワードと前記認証テーブル内の前記ユーザ名およびパスワードと照合するユーザ認証を実行し、前記ユーザ認証に成功したときのみ前記制御テーブルの更新および前記通信情報の授受を実行し、前記ユーザ認証に失敗したときは前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄する第 2 のステップと、

を実行することを特徴とする通信ネットワークシステムの管理方法。

【請求項 2】 請求項 1 記載の通信ネットワークシステムの管理方法において、

前記第 1 のステップでは、前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方に対して、前記ユーザおよび通信ネットワークシステムの管理者の少なくとも一方の連絡先メールアドレスも対応付けて設定し、前記第 2 のステップでは、前記ユーザ認証にて前記通信情報の送信元または送信先の前記ユーザから入力された前記ユーザ名を含むとともに前記制御テーブルの更新要求が発生したことを通知するメッセージを作成して該当する前記ネットワーク論理アドレスまたはネットワーク物理アドレスの前記ユーザおよび管理者の少なくとも一方の連絡先メールアドレスに対して送出する処理、

前記第 2 のステップでの前記ユーザ認証に失敗したとき、前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄し、さらに当該通信情報を受信した前記入出力ポートの切り離し、および当該入出力ポートから受信した全ての通信情報を廃棄する処理、

前記第 2 のステップでの前記ユーザ認証に失敗したとき、前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄し、さらに該通信情報の送信元の前記ネットワーク論理アドレスまたはネットワーク物理アドレスと同一の仮想 LAN（ローカル・エリア・ネットワーク）に属す全ての前記ネットワーク端末のユーザに、前記ネットワーク論理アドレスまたはネットワーク物理アドレス等の設定ミスや、悪意のユーザが他のネットワーク端末のアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して送る処理、

前記制御テーブルの更新要求発生の有無に関係なく、定期的または不定期に前記制御テーブル内に登録された前記ネットワーク論理アドレスまたはネットワーク物理アドレスのユーザに対して前記ユーザ認証を実行する処理、

の少なくとも一つの処理を実行することを特徴とする通信ネットワークシステムの管理方法。

【請求項 3】 ネットワーク端末またはネットワーク中継装置が接続される複数の入出力ポートと、個々の前記入出力ポートと前記ネットワーク端末または

ネットワーク中継装置に付与されたネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方を対応付けて格納する制御テーブルと、前記制御テーブルに基づいて複数の前記入出力ポートの各々に接続された前記ネットワーク端末またはネットワーク中継装置の相互間での通信情報の授受を行うとともに、前記通信情報に含まれる前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と前記入出力ポートとの対応関係の変化を学習して前記制御テーブルを更新することで、前記入出力ポートに対する前記ネットワーク端末またはネットワーク中継装置の接続状態の動的な変更を可能にする中継処理手段とを含む情報中継装置であって、

個々のネットワーク端末に対応した前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と、当該ネットワーク端末のユーザ名およびパスワードと、前記ユーザおよび通信ネットワークシステムの管理者の少なくとも一方の連絡先メールアドレスが対応付けて格納された認証テーブルと、

前記制御テーブルの更新を伴う前記通信情報の授受が発生した時、前記通信情報の授受および前記制御テーブルの更新に先立って、前記通信情報の送信元および送信先の少なくとも一方の前記ユーザに対して、ユーザ名およびパスワードの入力を要求し、入力されたユーザ名およびパスワードと前記認証テーブル内の前記ユーザ名およびパスワードと照合するユーザ認証を実行するとともに、前記通信情報の送信元および前記管理者の少なくとも一方の前記連絡先メールアドレスに対して前記ユーザ認証で得られた前記ユーザ名と前記制御テーブルの更新要求が発生したことを通知するメッセージを送信するとともに、前記ユーザ認証に成功したときのみ前記制御テーブルの更新および前記通信情報の授受を実行し、前記ユーザ認証に失敗したときは前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄する動作を行う制御論理と、

を備えたことを特徴とする情報中継装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信ネットワークシステムの管理技術および情報中継技術に関し、

特に、LAN (LAN: Local Area Network) スイッチ (Layer2 スイッチ、Layer3 スイッチ等) と呼ばれるインターネットワーク装置、およびLAN スイッチで構成する通信ネットワークシステム (LAN スイッチネットワークシステム) の管理方法等に適用して有効な技術に関する。

【0002】

【従来の技術】

LAN スイッチが有する特徴技術に VLAN (VLAN: Virtual LAN) がある。VLAN はインターネットワーク装置の物理的なポートに依存せずに LAN の構築を可能にする技術であり、その形式の違いによってポートベース VLAN、MAC (MAC: Media Access Control) アドレスベース VLAN、Layer3 プロトコルベース VLAN、IP (IP: Internet Protocol) サブネットベース VLAN 等の名称で知られている。

【0003】

本発明の参考技術では、例えば図7に示す IP サブネットベース VLAN の通信ネットワークシステムにおいて複数のポート 221 ~ 225 を備えた LAN スイッチ 210 は PC (PC: Personal Computer) 231 から PC 233 へのパケットを受信すると、パケットの始点 MAC アドレス、終点 MAC アドレス、始点 IP アドレスを学習してホストテーブル 220 を作成する。次に終点 IP アドレスをキーにホストテーブル 220 を参照し、該当エントリが有る場合は、該当ポートにパケットを出力する。該当エントリが無い場合は、ルーティングテーブル (図示無し) および ARP (ARP: Address Resolution Protocol) テーブル (図示無し) を参照してネクストホップを決め、該当するホストテーブル 220 のエントリを新規に作成して、該当ポートにパケットを出力する。LAN スイッチ 210 はこのようにして PC 231 から PC 233 へのパケットを中継する。

【0004】

さらに LAN スイッチ 210 では、定期的にホストテーブル 220 のエントリを廃棄し、新たにパケットから学習することによって常にホストテーブル 220 のエントリを更新しているため、PC が移動した場合でも移動先のポートにパケットを正しく中継することができる。すなわち PC は移動した場合でも移動前と

同様の通信を自動的に再開することができる。

【0005】

【発明が解決しようとする課題】

しかしながら、上記参考技術には、次の技術的課題がある。

【0006】

第1の技術的課題は、IPアドレス等の設定ミスに対して無防備なことである。例えばPC232がPC231のIPアドレスを誤って設定、ポート222に接続してしまったとする。この場合、LANスイッチ210ではPC231がポート221からポート222に移動したと判断し、そのようにホストテーブル220を書き換えてしまう。この結果、IPアドレスを正しく使用しているPC231が通信出来なくなる等の通信不良が発生する。また、ネットワークに接続されるPCの数が多い場合には、この通信不良の解析や回復には、多大の労力を要する。

【0007】

第2の技術的課題は、悪意のユーザによる盗聴やなりすましを許してしまうことである。例えばPC235がPC231のIPアドレスを設定、ポート225に接続したとする。この場合、LANスイッチ210ではPC231がポート221からポート225に移動したと判断し、そのようにホストテーブル220を書き換えてしまう。この結果、PC235がPC231宛の通信データを受け取って盗聴したり、またPC231になりすまして通信できてしまう。

【0008】

本発明の目的は、論理的あるいは物理的なネットワークアドレス等の設定ミスによる通信不良の防止や通信不良の原因解析および回復操作の迅速化が可能な通信ネットワークシステムの管理技術および情報中継技術を提供することにある。

【0009】

本発明の他の目的は、悪意のユーザによる盗聴やなりすましを防ぐことで通信ネットワークシステムのセキュリティを向上させることが可能な通信ネットワークシステムの管理技術および情報中継技術を提供することにある。

## 【0010】

## 【課題を解決するための手段】

本発明は、LANスイッチ等の情報中継装置に備えられた複数の入出力ポートにユーザ端末や他の中継装置を接続して構築され、入出力ポートに対するユーザ端末等の接続状態の変化を学習して、入出力ポートとネットワークアドレスとの対応関係を管理する制御テーブルを更新することで、個々のユーザ端末の入出力ポートに対する接続状態を動的に変更することが可能な通信ネットワークの管理方法において、各ユーザ端末間、すなわち複数の入出力ポート間で通信情報の授受を契機とする制御テーブルの更新要求が発生した時、当該通信情報の送信元のユーザ端末に対してユーザ認証を実行し、真正のユーザであることが確認された場合にのみ、制御テーブルの更新およびそれに基づく通信情報の授受を行わせるものである。

## 【0011】

また、各ユーザ端末およびシステム管理者の連絡先メールアドレスを、ユーザ認証に用いられるネットワークアドレスやユーザ名、パスワード等が格納された認証テーブルの一部に登録しておき、制御テーブルの更新要求の発生時に、当該更新要求が発生したことを記したメッセージを通信情報の送信元のユーザ端末やシステム管理者等にメールで送るものである。この際、ユーザ認証の成功の有無に関係なく、当該ユーザ認証にて得られたユーザ名を当該メッセージ内に格納する。

## 【0012】

より具体的には、本発明は、以下の特徴を有する。

## 【0013】

第1の観点では、本発明は、LANスイッチで構成する通信ネットワークシステムにおいて、IPアドレス等の設定ミスによる通信不良、悪意のユーザによる盗聴やなりすましを防ぐことができるLANスイッチネットワークシステムの管理方法であって、例えば図1に示すIPサブネットベースVLANの通信ネットワークシステムにおいて、(a) PC31～34はLANスイッチ11に予めIPアドレスとそのユーザ名、パスワード、連絡先メールアドレスを登録し、(b

）LANスイッチ11の管理者も同様にLANスイッチ11に予め連絡先メールアドレスを登録し、（c）LANスイッチは前記PC31～34および前記LANスイッチ11の管理者の情報を登録する認証テーブル16を作成し、（d）さらにLANスイッチ11はPC31からPC33へのパケットを受信すると、パケットの始点MACアドレス、終点MACアドレス、始点IPアドレスを学習してホストテーブル14（図2）を作成し、このとき前記ホストテーブル14の中に前記始点IPアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該パケットの受信ポートで且つ該パケットの始点IPアドレスのPCにユーザ名とパスワードを要求するとともに、ユーザ名とパスワードが返されるのを待って、前記認証テーブル16の中の前記始点IPアドレスに該当する連絡先メールアドレスにホストテーブル14の書き換え要求が発生した旨を伝えるメッセージ（本メッセージの中にPCから返されたユーザ名を情報として入れる。）を送り、さらに予め認証テーブル16に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、ホストテーブル14のエントリ書き換えを中止するとともに該パケットを廃棄し、予め認証テーブル16に登録されているユーザ名とパスワードが得られた場合は、終点IPアドレスをキーにホストテーブル14を参照し、該当エントリが有る場合は、該当ポートにパケットを出力し、該当エントリが無い場合は、ルーティングテーブル（図示無し）およびARPテーブル（図示無し）を参照してネクストホップを決め、該当するホストテーブル14のエントリを新規に作成して、該当ポートにパケットを出力することを特徴とするLANスイッチネットワークシステムの管理方法を提供する。

#### 【0014】

上記第1の観点によるLANスイッチネットワークシステムの管理方法では、PC31はポート21から他のポートに移動した場合でも移動前と同様の通信を自動的に再開することができるが、その際、LANスイッチ11から予め登録したユーザ名とパスワードの入力を求められるため、そのパスワードを知っているPC31以外がPC31を装って盗聴したり、なりすましたりすることが出来なくなる。またPC32がPC31のIPアドレスを誤って設定、ポート22に接

続してしまった場合でも、PC 31 および LAN スイッチ 11 の管理者にその旨を伝えるメッセージ（本メッセージの中に PC 32 のユーザ名が入れている）が送られるので、PC 31 のユーザや LAN スイッチ 11 の管理者は容易に障害原因の切り分け（解析）を行うことができ、迅速な回復処理が可能になる。

【0015】

第2の観点では、本発明は、（a）各ポート 21～25 との間でパケットの送受信を行う通信処理手段 12 と、（b）前記通信処理手段 12 から渡されたパケットの始点 MAC アドレス、終点 MAC アドレス、始点 IP アドレスを学習してホストテーブル 14（図2）を作成し、このとき前記ホストテーブル 14 の中に前記始点 IP アドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、書き換えて（新規作成も含む）良いか認証処理手段 15 に問い合わせ、その結果、書き換え禁止の通知を受けた場合は、前記ホストテーブル 14 のエントリ書き換えを中止するとともに該パケットを廃棄し、書き換え許可の通知を受けた場合は、終点 IP アドレスをキーに前記ホストテーブル 14 を参照し、該当エントリが有る場合は、該当ポートへのパケット出力を前記通信処理手段 12 に指示し、該当エントリが無い場合は、ルーティングテーブル（図示無し）および ARP テーブル（図示無し）を参照してネクストホップを決め、前記ホストテーブル 14 に該当するエントリを新規に作成して、該当ポートへのパケット出力を前記通信処理手段 12 に指示する中継処理手段 13 と、（c）予め管理端末（図示無し）等を介して入力された各 PC 31～34 の IP アドレス、ユーザ名、パスワード、連絡先メールアドレス等を登録して認証テーブル 16 を作成し、前記中継処理手段 13 から指示されると、指示された IP アドレスの PC にユーザ名とパスワードの入力を要求するメッセージを作成して、該パケットの受信ポートへの送出を前記通信処理手段 12 に指示するとともに、ユーザ名とパスワードが返されるのを待って、前記認証テーブル 16 の中の前記 IP アドレスに該当する連絡先メールアドレスにホストテーブル 14 のエントリ書き換え要求が発生した旨を伝えるメッセージ（本メッセージの中に PC から返されたユーザ名を情報として入れる）を作成して前記通信処理手段 12 に送出を指示し、さらに予め認証テーブル 16 に登録されているユーザ名とパスワ

ードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル 14 のエントリの書き換え禁止を前記中継処理手段 13 に通知し、予め認証テーブル 16 に登録されているユーザ名とパスワードが得られた場合は、前記ホストテーブル 14 のエントリの書き換え許可を前記中継処理手段 13 に通知する認証処理手段 15 とを具備したことを特徴とする LAN スイッチ 11 を提供する。

## 【0016】

上記第 2 の観点による LAN スイッチ 11 によれば、上記第 1 の観点の LAN スイッチネットワークシステムの管理方法を好適に実施できるようになる。

## 【0017】

第 3 の観点では、本発明は、上記構成の LAN スイッチ 11 において、前記認証処理手段 15 は、前記中継処理手段 13 から指示されたホストテーブル 14 のエントリの IP アドレスの PC にユーザ名とパスワードの入力を要求するメッセージを作成して、該パケットの受信ポートへの送出を前記通信処理手段 12 に指示し、予め認証テーブル 16 に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル 14 のエントリの書き換え禁止を前記中継処理手段 13 に通知するだけでなく、該パケットを受信したポートの切り離しや該ポートから受信する全てのパケットの廃棄を前記中継処理手段 13 に指示することを特徴とする LAN スイッチ 11 を提供する。

## 【0018】

上記第 3 の観点による LAN スイッチ 11 によれば、IP アドレス等の設定ミスや悪意のユーザが他の PC のアドレスを使って盗聴やなりすまして通信を行おうとすることによるユーザ名とパスワードの入力要求の繰り返しのトラヒック負荷を減らすことができる。

## 【0019】

第 4 の観点では、本発明は、上記構成の LAN スイッチ 11 において、前記認証処理手段 15 は、前記中継処理手段 13 から指示されたホストテーブル 14 のエントリの IP アドレスの PC にユーザ名とパスワードの入力を要求するメッセ

ージを作成して、該パケットの受信ポートへの送出を前記通信処理手段 12 に指示し、予め認証テーブル 16 に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル 14 のエントリの書き換え禁止を前記中継処理手段 13 に通知するだけでなく、該パケットの始点 IP アドレスと同一 VLAN に属す全ての PC のユーザに、IP アドレス等の設定ミスや悪意のユーザが他の PC のアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して、前記通信処理手段 12 に指示して送出させることを特徴とする LAN スイッチ 11 を提供する。

#### 【0020】

また、第 4 の観点の別の側面として、本発明は、上記構成の LAN スイッチ 11 において、前記認証処理手段 15 は、前記中継処理手段 13 から指示されたホストテーブル 14 のエントリの IP アドレスの PC にユーザ名とパスワードの入力を要求するメッセージを作成して、該パケットの受信ポートへの出力を前記通信処理手段 12 に指示し、予め認証テーブル 16 に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）のみ、前記認証テーブル 16 の中の前記始点 IP アドレスに該当する連絡先メールアドレスにホストテーブル 14 の書き換え失敗が発生した旨を伝えるメッセージを作成して、前記通信処理手段 12 に指示して送出させることを特徴とする LAN スイッチ 11 を提供する。

#### 【0021】

上記第 4 の観点による前者の LAN スイッチ 11 によれば、IP アドレス等の設定ミスや悪意のユーザが他の PC のアドレスを使って盗聴やなりすましの通信を行おうとしていることを、当事者だけでなく、その後同じ事が起きる可能性があるユーザにも事前に警告を発することができる。

#### 【0022】

また上記第 4 の観点による後者の LAN スイッチ 11 によれば、書き換え成功時（真正なユーザが正常な使用範囲で通信している場合）に真正なユーザに送られてくるメールを無くしてトラフィック量を減らすとともに、書き換えに失敗する

場合のみ、その旨を伝えることによって、より迅速な障害原因の切り分け（解析）および回復処理が可能となる。

【0023】

第5の観点では、本発明は、上記構成のLANスイッチ11において、前記認証処理手段15は、ホストテーブル14のエントリの新規作成時や書き換え時ではなく、各エントリについて定期的にユーザ名とパスワードの問い合わせを行うことを特徴とするLANスイッチ11を提供する。

【0024】

上記第5の観点によるLANスイッチ11によれば、パケットを受信するのみで自ら発信を行わないPCについても、IPアドレス等の設定ミスをしていないか、悪意のユーザが他のPCのアドレスを使って盗聴やなりすましの通信を行っていないかチェックすることができる。

【0025】

また上記第5の観点によるLANスイッチによれば、ポート接続ミス・IPアドレス設定ミス等や、悪意のユーザが、それまで真正なユーザのPCが接続していたポートに、その真正なユーザのIPアドレスを設定してPCを接続し、盗聴やなりすましの通信を行っていないかチェックすることができる。

【0026】

第6の観点では、本発明は、上記構成のLANスイッチ11において、前記中継処理手段13は、受信パケットの始点IPアドレスに該当するホストテーブル14のエントリの新規作成時や書き換えが発生した場合に、それを書き換えて良いか前記認証処理手段15に問い合わせるだけでなく、受信パケットの終点IPアドレスについても同様に、該当するホストテーブル14のエントリの新規作成時や書き換えが発生した場合に、それを書き換えて良いか前記認証処理手段15に問い合わせることを特徴とするLANスイッチ11を提供する。

【0027】

上記第6の観点によるLANスイッチ11によれば、パケットを受信するのみで自ら発信を行わないPCについても、IPアドレス等の設定ミスをしていないか、悪意のユーザが他のPCのアドレスを使って盗聴やなりすましの通信を行っ

ていないかチェックすることができる。

【0028】

また上記第6の観点によるLANスイッチによれば、ポート接続ミス・IPアドレス設定ミス等や、悪意のユーザが、それまで真正なユーザのPCが接続していたポートに、その真正なユーザのIPアドレスを設定してPCを接続し、盗聴やなりすましの通信を行っていないかチェックすることができる。

【0029】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照しながら詳細に説明する。なお、これにより本発明が限定されるものではない。

【0030】

図1は、本発明の第1の実施形態である通信ネットワークシステムの管理方法を実施するLANスイッチの構成、および当該LANスイッチが適用されるIPサブネットベースVLANの一例を示す概念図である。また、図2および図3は、本実施の形態のLANスイッチにて用いられる各種制御情報の一例を示す概念図、図4、図5および図6は、本実施の形態の通信ネットワークシステムの管理方法およびLANスイッチの作用の一例を示すフローチャートである。

【0031】

本実施の形態のLANスイッチ11は、受信したパケット（通信情報）から学習して作成した図2のようなホストテーブル14に基づき各ポート21～25間のパケットの中継を行うことにより、PC31～34の間の通信を実現するものであり、通信処理手段12と、中継処理手段13と、認証処理手段15とから構成される。

【0032】

前記通信処理手段12は、各ポート21～25との間でパケットの送受信を行う手段であり、例えばCPU、ASIC、RAM、ROM等の電子デバイスで構成される。

【0033】

前記中継処理手段13は、ホストテーブル14に基づき各ポート21～25間

のパケットの中継を行う手段であり、例えばCPU、ASIC、RAM、ROM等の電子デバイスで構成される。

【0034】

図2に例示されるように、ホストテーブル14は、始点IPアドレス14a、始点MACアドレス14b、終点MACアドレス14c、ポート番号14d、当該ポートが帰属するVLAN等のネットワークを示す帰属ネットワーク14e、等の情報が対応付けられて格納されている。

【0035】

前記認証処理手段15は、ホストテーブル14の書き換え可否の判定を行う手段であり、例えばCPU、ASIC、RAM、ROM等の電子デバイスで構成される。書き換え可否の判定の基となる情報は認証テーブル16（後述）に予め登録、保持している。

【0036】

図3は、本実施の形態のLANスイッチ11にて用いられる認証テーブル16の構成図である。認証テーブル16には、PC31～34のIPアドレス16aと、そのPCを使用しているユーザ名16b、パスワード16c、連絡先メールアドレス16dが予めコンソール端末（図示無し）等を介して登録されている。

【0037】

先ず、PC31からPC33に通信する場合の動作について説明する。

【0038】

図4は、PC31からPC33に通信する場合の本実施の形態のLANスイッチ11および通信ネットワークシステムの管理方法の動作の一例を示すフローチャートである。

【0039】

なお各PC31～34はLANスイッチ11に予めIPアドレスとそのユーザ名、パスワード、連絡先メールアドレスを登録し、LANスイッチ11の管理者も同様にLANスイッチ11に予め連絡先メールアドレスを登録し、LANスイッチ11は前記PC31～34および前記LANスイッチ11の管理者の情報を登録する認証テーブル16を作成してあるものとする。

【0040】

PC31は、PC33宛のパケットを作成してポート21に送出する（ステップ101）。

【0041】

LANスイッチ11の通信処理手段12は、前記パケットをポート21から受信処理して中継処理手段13に渡す（ステップ102）。

【0042】

中継処理手段13は、受信パケットの始点MACアドレス、終点MACアドレス、始点IPアドレスを学習してホストテーブル14を作成する。このときホストテーブル14の中に前記始点IPアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該エントリを書き換えて（新規作成も含む）良いか認証処理手段15に問い合わせる（ステップ103）。書き換える必要（新規作成も含む）が無い場合はステップ110に進む。本ケースは通信開始の1パケット目のケースであり、新規作成するため次ステップに進むものとする。2パケット目以降のケースではステップ110に進む。

【0043】

認証処理手段15は、ユーザ名とパスワードの入力要求メッセージ（メッセージAと呼ぶ。）を作成して通信処理手段12に送出を指示した後、一定時間待つ（ステップ104）。

【0044】

通信処理手段12は、メッセージAを該パケットの受信ポート（この場合、ポート21）の該IPアドレス宛に送出する（ステップ105）。

【0045】

通信処理手段12は、メッセージAの応答メッセージ、すなわちユーザ名とパスワードの入力メッセージ（メッセージBと呼ぶ。）をPC31から受信すると、受信処理して認証処理手段15に渡す（ステップ106）。

【0046】

認証処理手段15は、メッセージBに格納されているIPアドレス、ユーザ名、パスワードと、認証テーブル16に書かれているIPアドレス16a、ユーザ

名 16 b、パスワード 16 c を比較して一致することを確認した後、認証テーブル 16 の該当エントリに登録されている連絡先メールアドレス 16 d にホストテーブル 14 の書き換え要求が発生した旨を伝えるメッセージ（メッセージ C と呼ぶ。メッセージ C の中にはメッセージ B に格納されているユーザ名を情報として入れる。）を作成して通信処理手段 12 に送出を指示する（ステップ 107）とともに、書き換え許可の旨を中継処理手段 13 に通知する（ステップ 109）。

【0047】

通信処理手段 12 は、メッセージ C を該メールアドレス宛に送出する（ステップ 108）。

【0048】

一方、中継処理手段 13 は、認証処理手段 15 から書き換え許可の旨の通知を受けると、ホストテーブル 14 の該当エントリの書き換えを行い、次に終点 IP アドレスをキーにホストテーブル 14 を参照し、該当エントリが有る場合は、該当ポートへのパケット出力を通信処理手段 12 に指示し、該当エントリが無い場合は、ルーティングテーブル（図示無し）および ARP テーブル（図示無し）を参照してネクストホップを決め、該当するホストテーブル 14 のエントリを新規に作成して、該当ポートへのパケット出力を通信処理手段 12 に指示する（ステップ 110）。

【0049】

通信処理手段 12 は、該パケットを該当ポートに送出する（ステップ 111）。

【0050】

以上により、PC 31 から PC 33 への通信を開始することが出来る。

【0051】

次に PC 31 がポート 21 からポート 25 に移動した後、PC 33 に通信する場合の動作について説明する。

【0052】

PC 31 の IP アドレスに該当するエントリが既にホストテーブル 14 にできている点が前述のケースと異なるが、動作は図 4 に示すフローチャートと同じ動

きをする。

【0053】

PC31は、PC33宛のパケットを作成してポート21に送出する（ステップ101）。

【0054】

LANスイッチ11の通信処理手段12は、前記パケットを受信処理して中継処理手段13に渡す（ステップ102）。

【0055】

中継処理手段13は、受信パケットの始点MACアドレス、終点MACアドレス、始点IPアドレスを学習してホストテーブル14を作成する。このときホストテーブル14の中に前記始点IPアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該エントリを書き換えて（新規作成も含む）良いか認証処理手段15に問い合わせる（ステップ103）。書き換える必要（新規作成も含む）が無い場合はステップ110に進む。本ケースは移動後の通信再開の1パケット目のケースであり、エントリの情報を書き換えるため次ステップに進むものとする。2パケット目以降のケースではステップ110に進む。

【0056】

認証処理手段15は、ユーザ名とパスワードの入力要求メッセージ（メッセージAと呼ぶ。）を作成して通信処理手段12に送出を指示した後、一定時間待つ（ステップ104）。

【0057】

通信処理手段12は、メッセージAを該パケットの受信ポートの該IPアドレス宛に送出する（ステップ105）。

【0058】

通信処理手段12は、メッセージAの応答メッセージ、すなわちユーザ名とパスワードの入力メッセージ（メッセージBと呼ぶ。）を受信すると、受信処理して認証処理手段15に渡す（ステップ106）。

## 【0059】

認証処理手段15は、メッセージBに格納されているIPアドレス、ユーザ名、パスワードと、認証テーブル16に書かれているIPアドレス16a、ユーザ名16b、パスワード16cを比較して一致することを確認した後、認証テーブル16の該当エントリに登録されている連絡先メールアドレス16dにホストテーブル14の書き換え要求が発生した旨を伝えるメッセージ（メッセージCと呼ぶ。メッセージCの中にはメッセージBに格納されているユーザ名を情報として入れる。）を作成して通信処理手段12に送出を指示する（ステップ107）とともに、書き換え許可の旨を中継処理手段13に通知する（ステップ109）。

## 【0060】

通信処理手段12は、メッセージCを該メールアドレス宛に送出する（ステップ108）。

## 【0061】

一方、中継処理手段13は、認証処理手段15から書き換え許可の旨の通知を受けると、ホストテーブル14の該当エントリの書き換えを行い、次に終点IPアドレスをキーにホストテーブル14を参照し、該当エントリが有る場合は、該当ポートへのパケット出力を通信処理手段12に指示し、該当エントリが無い場合は、ルーティングテーブル（図示無し）およびARPテーブル（図示無し）を参照してネクストホップを決め、該当するホストテーブル14のエントリを新規に作成して、該当ポートへのパケット出力を通信処理手段12に指示する（ステップ110）。

## 【0062】

通信処理手段12は、該パケットを該当ポート（この場合、ポート25）に送出する（ステップ111）。

## 【0063】

以上により、PC31はポート21からポート25へ移動後も、PC33との通信を自動的に再開することが出来る。

## 【0064】

次にPC32がPC31のIPアドレスを誤って設定、ポート22に接続して

しまい、PC33との通信を開始した場合の動作について説明する。

【0065】

図5は、PC32がPC31のIPアドレスを誤って設定、ポート22に接続してしまい、PC33との通信を開始した場合における、本実施の形態のLANスイッチ11および通信ネットワークシステムの管理方法の動作の一例を示すフローチャートである。

【0066】

PC32は、PC33宛のパケットを作成してポート21に送出する（ステップ121）。

【0067】

LANスイッチ11の通信処理手段12は、前記パケットを受信処理して中継処理手段13に渡す（ステップ102）。

【0068】

中継処理手段13は、受信パケットの始点MACアドレス、終点MACアドレス、始点IPアドレスを学習してホストテーブル14を作成する。このときホストテーブル14の中に前記始点IPアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該エントリを書き換えて（新規作成も含む）良いか認証処理手段15に問い合わせる（ステップ103）。書き換える必要（新規作成も含む）が無い場合はステップ110に進む。本ケースはPC32がPC31のIPアドレスを誤って設定、ポート22に接続してしまい、PC33との通信を開始した1パケット目のケースであり、エントリの情報を書き換えるため次ステップに進むものとする。なお本ケースでは結果としてエントリの情報の書き換えに失敗するため、2パケット目以降のケースも次ステップに進むことになる。

【0069】

認証処理手段15は、ユーザ名とパスワードの入力要求メッセージ（メッセージAと呼ぶ。）を作成して通信処理手段12に送出を指示した後、一定時間待つ（ステップ104）。

【0070】

通信処理手段12は、メッセージAを該パケットの受信ポート（この場合、ポート22）の該IPアドレス宛に送出する（ステップ105）。

【0071】

通信処理手段12は、メッセージAの応答メッセージ、すなわちユーザ名とパスワードの入力メッセージ（メッセージBと呼ぶ。）を受信すると、受信処理して認証処理手段15に渡す（ステップ106）。

【0072】

認証処理手段15は、メッセージBに格納されているIPアドレス、ユーザ名、パスワードと、認証テーブル16に書かれているIPアドレス16a、ユーザ名16b、パスワード16cを比較して一致していないことを確認した後、認証テーブル16の該当エントリに登録されている連絡先メールアドレス16dにホストテーブル14の書き換え要求が発生した旨を伝えるメッセージ（メッセージCと呼ぶ。メッセージCの中にはメッセージBに格納されているユーザ名を情報として入れる。）を作成して通信処理手段12に送出を指示する（ステップ108）とともに、書き換え禁止の旨を中継処理手段13に通知する（ステップ122）。

【0073】

通信処理手段12は、メッセージCを該メールアドレス宛に送出する（この場合、メッセージCは、PC32において謝って設定されたIPアドレスの真正の所有者であるPC31宛にメッセージCが送られる。）（ステップ108）。

【0074】

一方、中継処理手段13は、認証処理手段15から書き換え禁止の旨の通知を受けると、ホストテーブル14の該当エントリの書き換えを中止し、該パケットを廃棄する（ステップ123）。

【0075】

以上により、PC32がPC31のIPアドレスを誤って設定、ポート22に接続してしまった場合でも、真正のPC31およびLANスイッチ11の管理者にその旨を伝えるメッセージ（本メッセージの中に誤設定操作を行ったPC32

のユーザ名が入れている) が送られるので、PC31のユーザやLANスイッチ11の管理者は容易に障害原因の切り分けを行うことができ、迅速な回復処理が可能となる。

## 【0076】

次に悪意のユーザのPC35がPC31のIPアドレスを設定、ポート25に接続し、PC33との通信を開始した場合の動作について説明する。

## 【0077】

図6は、悪意のユーザのPC35がPC31のIPアドレスを設定、ポート25に接続し、PC33との通信を開始した場合における、本実施の形態のLANスイッチ11および通信ネットワークシステムの管理方法の動作の一例を示すフローチャートである。

## 【0078】

PC35は、PC33宛のパケットを作成してポート25に送出する(ステップ131)。

## 【0079】

LANスイッチ11の通信処理手段12は、前記パケットを受信処理して中継処理手段13に渡す(ステップ102)。

## 【0080】

中継処理手段13は、受信パケットの始点MACアドレス、終点MACアドレス、始点IPアドレスを学習してホストテーブル14を作成する。このときホストテーブル14の中に前記始点IPアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該エントリを書き換えて(新規作成も含む)良いか認証処理手段15に問い合わせる(ステップ103)。書き換える必要(新規作成も含む)が無い場合はステップ110に進む。本ケースは悪意のユーザのPC35がPC31のIPアドレスを設定、ポート25に接続し、PC33との通信を開始した1パケット目のケースであり、エントリの情報を書き換えるため次ステップに進むものとする。なお本ケースでは結果としてエントリの情報の書き換えに失敗するため、2パケット目以降のケースも次ステップに進むことになる。

## 【0081】

認証処理手段15は、ユーザ名とパスワードの入力要求メッセージ（メッセージAと呼ぶ。）を作成して通信処理手段12に送出を指示した後、一定時間待つ（ステップ104）。

## 【0082】

通信処理手段12は、メッセージAを該パケットの受信ポート（この場合、ポート25）の該IPアドレス宛に送出する（ステップ105）。

## 【0083】

通信処理手段12は、メッセージAの応答メッセージ、すなわちユーザ名とパスワードの入力メッセージ（メッセージBと呼ぶ。）を受信すると、受信処理して認証処理手段15に渡す（ステップ106）。

## 【0084】

認証処理手段15は、メッセージBに格納されているIPアドレス、ユーザ名、パスワードと、認証テーブル16に書かれているIPアドレス16a、ユーザ名16b、パスワード16cを比較して一致していないことを確認した後、認証テーブル16の該当エントリに登録されている連絡先メールアドレス16dにホストテーブル14の書き換え要求が発生した旨を伝えるメッセージ（メッセージCと呼ぶ。メッセージCの中にはメッセージBに格納されているユーザ名を情報として入れる。メッセージBにユーザ名が入れられてない場合や一定時間内にメッセージBが送られてこなかった場合はその旨を伝える情報を入れる。）を作成して通信処理手段12に送出を指示する（ステップ122）とともに、書き換え禁止の旨を中継処理手段13に通知する（ステップ109）。

## 【0085】

通信処理手段12は、メッセージCを該メールアドレス宛に送出する（この場合、メッセージCは、パケットの送信元のPC35ではなく、真正のユーザであるPC31に届く）（ステップ108）。

## 【0086】

一方、中継処理手段13は、認証処理手段15から書き換え禁止の旨の通知を受けると、ホストテーブル14の該当エントリの書き換えを中止し、該パケット

を廃棄する（ステップ 123）。

【0087】

また、メッセージ C を受け取ったシステムの管理者は、メッセージ C に格納されている情報に基づいて事態を把握し、対策をとることができる。

【0088】

以上により、悪意のユーザの PC 35 が PC 31 の IP アドレスを設定し、ポート 25 に接続しても、PC 35 は予め PC 31 が LAN スイッチ 11 に登録したユーザ名とパスワードの入力を求められ、それに正しく応えられないため、ホストテーブル 14 の書き換えは行われず、したがって PC 35 が PC 31 を装って盗聴したり、なりすましたりすることを防ぐことができる。

【0089】

次に、第 1 の実施例とは別の実施例について説明する。

【0090】

第 1 の実施例では LAN スイッチ 11 において、認証処理手段 15 は、中継処理手段 13 から指示されたホストテーブル 14 のエントリの IP アドレスの PC にユーザ名とパスワードの入力を要求するメッセージ A を作成して、該パケットの受信ポートへの送出を通信処理手段 12 に指示し、予め認証テーブル 16 に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル 14 のエントリの書き換え禁止を前記中継処理手段 13 に通知しているが、さらにそれに加えて該パケットを受信したポートの切り離し（閉塞）や該ポートから受信する全てのパケットの廃棄を前記中継処理手段 13 に指示するようにしても良い。以上により、IP アドレス等の設定ミスや悪意のユーザが他の PC のアドレスを使って盗聴やなりすまして通信を行おうとすることによるユーザ名とパスワードの入力要求の繰り返しのトラヒック負荷を減らすことができる。

【0091】

また、第 1 の実施例では LAN スイッチ 11 において、認証処理手段 15 は、中継処理手段 13 から指示されたホストテーブル 14 のエントリの IP アドレスの PC にユーザ名とパスワードの入力を要求するメッセージ A を作成して、該パ

ケットの受信ポートへの送出を通信処理手段 12 に指示し、予め認証テーブル 16 に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル 14 のエントリの書き換え禁止を前記中継処理手段 13 に通知しているが、さらにそれに加えて該パケットの始点 IP アドレスと同一 VLAN に属す全ての PC のユーザに、IP アドレス等の設定ミスや悪意のユーザが他の PC のアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して、前記通信処理手段 12 に指示して送出させても良い。以上により、IP アドレス等の設定ミスや悪意のユーザが他の PC のアドレスを使って盗聴やなりすましの通信を行おうとしていることを、当事者だけでなく、その後同じ事が起きる可能性があるユーザにも事前に警告を発することができる。

## 【0092】

また、第 1 の実施例では LAN スイッチ 11 において、認証処理手段 15 は、ホストテーブル 14 のエントリの新規作成や書き換えが発生し、中継処理手段 13 から書き換え（新規作成を含む）て良いか問い合わせを受けた時に該エントリの IP アドレスの PC にユーザ名とパスワードの入力を要求しているが、定期的に各エントリの IP アドレスの PC にユーザ名とパスワードの入力を要求して真正のユーザか否かを確認するユーザ認証を行っても良い。以上により、パケットを受信するのみで自ら発信を行わない PC についても、IP アドレス等の設定ミスをしていないか、悪意のユーザが他の PC のアドレスを使って盗聴やなりすましの通信を行っていないかチェックすることができる。

## 【0093】

また、第 1 の実施例では LAN スイッチ 11 において、中継処理手段 13 は、受信パケットの始点 IP アドレスに該当するホストテーブル 14 のエントリの新規作成時や書き換えが発生した場合に、それを書き換えて良いか認証処理手段 15 に問い合わせるだけでなく、受信パケットの終点 IP アドレスについても同様に、該当するホストテーブル 14 のエントリの新規作成時や書き換えが発生した場合に、それを書き換えて良いか前記認証処理手段 15 に問い合わせ、書き換え許可がおりた場合のみ該エントリを書き換えを行うようにしても良い。以上によ

り、パケットを受信するのみで自ら発信を行わないPCについても、IPアドレス等の設定ミスをしていないか、悪意のユーザが他のPCのアドレスを使って盗聴やなりすましの通信を行っていないかチェックすることができる。

【0094】

また、第1の実施例ではIPサブネットベースVLANの例を用いて説明しているが、ポートベースVLAN、MACアドレスベースVLAN、Layer3プロトコルベースVLAN等の他の形式のVLANでも同様である。

【0095】

以上のように、本発明の各実施の形態の通信ネットワークの管理方法およびLANスイッチによれば、悪意のユーザによる盗聴やなりすましを防ぐことができ、通信ネットワークシステムのセキュリティが向上する。

【0096】

また、ユーザ認証にて得られたユーザ名等の情報を真正のユーザやシステムの管理者にメールで通知することにより、IPアドレス等の設定ミスによる障害原因を容易に切り分けられるようになり、迅速な回復処理が可能になる。

【0097】

上記した特許請求の範囲に記載された以外の本発明の特徴を列挙すれば以下の通りである。

【0098】

すなわち、

<1> LANスイッチで構成する通信ネットワークシステムの管理方法であって、(a) 各PCはLANスイッチに予めIPアドレスとそのユーザ名、パスワード、連絡先メールアドレスを登録し、(b) LANスイッチの管理者も同様にLANスイッチに予め連絡先メールアドレスを登録し、(c) LANスイッチは前記PCおよび前記LANスイッチの管理者の情報を登録する認証テーブルを作成し、(d) さらにLANスイッチは各PC間の通信のパケットを受信すると、該パケットの始点MACアドレス、終点MACアドレス、始点IPアドレスを学習してホストテーブルを作成し、このとき前記ホストテーブルの中に前記始点IPアドレスに該当するエントリが無く新規に作成する場合や該当エントリと

異なる情報に書き換える場合は、該パケットの受信ポートで且つ該パケットの始点IPアドレスのPCにユーザ名とパスワードを要求するとともに、ユーザ名とパスワードが返されるのを待って、前記ホストテーブルの書き換え要求が発生した旨を伝えるメッセージを作成し、該メッセージの中にPCから返されたユーザ名を情報として入れ、前記認証テーブルの中の前記始点IPアドレスに該当する連絡先メールアドレスに送り、さらに予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合は、前記ホストテーブルのエントリ書き換えを中止するとともに該パケットを廃棄し、予め前記認証テーブルに登録されているユーザ名とパスワードが得られた場合は、終点IPアドレスをキーに前記ホストテーブルを参照し、該当エントリが有る場合は、該当ポートにパケットを出力し、該当エントリが無い場合は、該当するホストテーブルのエントリを新規に作成して、該当ポートにパケットを出力することを特徴とする通信ネットワークシステムの管理方法。

## 【0099】

＜2＞ 前記＜1＞記載の通信ネットワークシステムの管理方法において、LANスイッチは、予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合に、前記ホストテーブルのエントリ書き換えを中止し、該パケットを廃棄することに加えて、さらに該パケットを受信したポートの切り離しや該ポートから受信する全てのパケット廃棄を行うことを特徴とする通信ネットワークシステムの管理方法。

## 【0100】

＜3＞ 前記＜1＞記載の通信ネットワークシステムの管理方法において、LANスイッチは、予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合に、前記ホストテーブルのエントリ書き換えを中止し、該パケットを廃棄することに加えて、さらに該パケットの始点IPアドレスと同一VLANに属す全てのPCのユーザに、IPアドレス等の設定ミスや悪意のユーザが他のPCのアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して送ることを特徴とする通信ネットワークシステムの管理方法。

## 【0101】

<4> 前記<1>記載の通信ネットワークシステムの管理方法において、LANスイッチは、ホストテーブルのエントリ新規作成時や書き換えが発生した場合に該エントリのIPアドレスのPCにユーザ名とパスワードの入力を要求することに加えて、さらに定期的に各エントリのIPアドレスのPCにユーザ名とパスワードの入力を要求することを特徴とする通信ネットワークシステムの管理方法。

## 【0102】

<5> 前記<1>記載の通信ネットワークシステムの管理方法において、LANスイッチは、受信パケットの始点IPアドレスに該当するホストテーブルのエントリの新規作成時や書き換えが発生した場合に該エントリのIPアドレスのPCにユーザ名とパスワードの入力を要求することに加えて、さらに該パケットの終点IPアドレスに該当するホストテーブルのエントリの新規作成時や書き換えが発生した場合に該エントリのIPアドレスのPCにユーザ名とパスワードの入力を要求し、始点IPアドレスと同様に終点IPアドレスについても、予め認証テーブルに登録されているユーザ名とパスワードが得られた場合のみ該エントリの書き換えを行うことを特徴とする通信ネットワークシステムの管理方法。

## 【0103】

<6> (a) 各ポートとの間でパケットの送受信を行う通信処理手段と、  
(b) 前記通信処理手段から渡されたパケットの始点MACアドレス、終点MACアドレス、始点IPアドレスを学習してホストテーブルを作成し、このとき前記ホストテーブルの中に前記始点IPアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、新規作成または書き換えて良いか認証処理手段に問い合わせ、その結果、書き換え禁止の通知を受けた場合は、前記ホストテーブルのエントリ書き換えを中止するとともに該パケットを廃棄し、書き換え許可の通知を受けた場合は、終点IPアドレスをキーに前記ホストテーブルを参照し、該当エントリが有る場合は、該当ポートへのパケット出力を前記通信処理手段に指示し、該当エントリが無い場合は、前記ホストテーブルに該当するエントリを新規に作成して、該当ポートへのパケット出力

を前記通信処理手段に指示する中継処理手段と、(c) 予め管理端末等を介して入力された各PCのIPアドレス、ユーザ名、パスワード、連絡先メールアドレス等を登録して認証テーブルを作成し、前記中継処理手段から指示されると、指示されたIPアドレスのPCにユーザ名とパスワードの入力を要求するメッセージを作成して、前記パケットの受信ポートへの送出を前記通信処理手段に指示するとともに、ユーザ名とパスワードが返されるのを待って、前記認証テーブルの中の前記IPアドレスに該当する連絡先メールアドレスに前記ホストテーブルのエントリ書き換え要求が発生した旨を伝えるメッセージを作成し、該メッセージの中にPCから返されたユーザ名を情報として入れ、前記通信処理手段に送出を指示し、さらに予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合は、前記ホストテーブルのエントリの書き換え禁止を前記中継処理手段に通知し、予め認証テーブルに登録されているユーザ名とパスワードが得られた場合は、前記ホストテーブルのエントリの書き換え許可を前記中継処理手段に通知する認証処理手段とを具備したことを特徴とするLANスイッチ。

## 【0104】

<7> LANスイッチで構成する通信ネットワークシステムの管理方法であって、(a) 各PCはLANスイッチに予めMACアドレスとそのユーザ名、パスワード、連絡先メールアドレスを登録し、(b) LANスイッチの管理者も同様にLANスイッチに予め連絡先メールアドレスを登録し、(c) LANスイッチは前記PCおよび前記LANスイッチの管理者の情報を登録する認証テーブルを作成し、(d) さらにLANスイッチは各PC間の通信のパケットを受信すると、該パケットの始点MACアドレスを学習してホストテーブルを作成し、このとき前記ホストテーブルの中に前記始点MACアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該パケットの受信ポートで且つ該パケットの始点MACアドレスのPCにユーザ名とパスワードを要求するとともに、ユーザ名とパスワードが返されるのを待って、前記ホストテーブルの書き換え要求が発生した旨を伝えるメッセージを作成し、該メッセージの中にPCから返されたユーザ名を情報として入れ、前記認証テー

ブルの中の前記始点MACアドレスに該当する連絡先メールアドレスに送り、さらに予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合は、前記ホストテーブルのエントリ書き換えを中止するとともに該パケットを廃棄し、予め前記認証テーブルに登録されているユーザ名とパスワードが得られた場合は、終点MACアドレスをキーに前記ホストテーブルを参照し、該当エントリが有る場合は、該当ポートにパケットを出力し、該当エントリが無い場合は、該当するホストテーブルのエントリを新規に作成して、該当ポートにパケットを出力することを特徴とする通信ネットワークシステムの管理方法。

## 【0105】

以上本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

## 【0106】

## 【発明の効果】

本発明の通信ネットワークシステムの管理方法によれば、論理的あるいは物理的なネットワークアドレス等の設定ミスによる通信不良の防止や通信不良の原因解析および回復操作の迅速化が可能になる、という効果が得られる。

## 【0107】

また、本発明の通信ネットワークシステムの管理方法によれば、悪意のユーザによる盗聴やなりすましを防ぐことで通信ネットワークのセキュリティを向上させることができる、という効果が得られる。

## 【0108】

本発明の情報中継装置によれば、論理的あるいは物理的なネットワークアドレス等の設定ミスによる通信不良の防止や通信不良の解析および回復操作の迅速化が可能になる、という効果が得られる。

## 【0109】

また、本発明の情報中継装置によれば、悪意のユーザによる盗聴やなりすましを防ぐことで通信ネットワークシステムのセキュリティを向上させることができ

る、という効果が得られる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施形態である通信ネットワークシステムの管理方法を実施する LAN スイッチの構成の一例を示す概念図である。

【図 2】

本発明の第 1 の実施形態である通信ネットワークシステムの管理方法を実施する LAN スイッチにて用いられるホストテーブルの一例を示す概念図である。

【図 3】

本発明の第 1 の実施形態である通信ネットワークシステムの管理方法を実施する LAN スイッチにて用いられる認証テーブルの一例を示す概念図である。

【図 4】

本発明の第 1 の実施形態である通信ネットワークシステムの管理方法を実施する LAN スイッチの作用の一例を示すフローチャートである。

【図 5】

本発明の第 1 の実施形態である通信ネットワークシステムの管理方法を実施する LAN スイッチの作用の一例を示すフローチャートである。

【図 6】

本発明の第 1 の実施形態である通信ネットワークシステムの管理方法を実施する LAN スイッチの作用の一例を示すフローチャートである。

【図 7】

本発明の参考技術である IP サブネットベース VLAN の一例を示す概念図である。

【符号の説明】

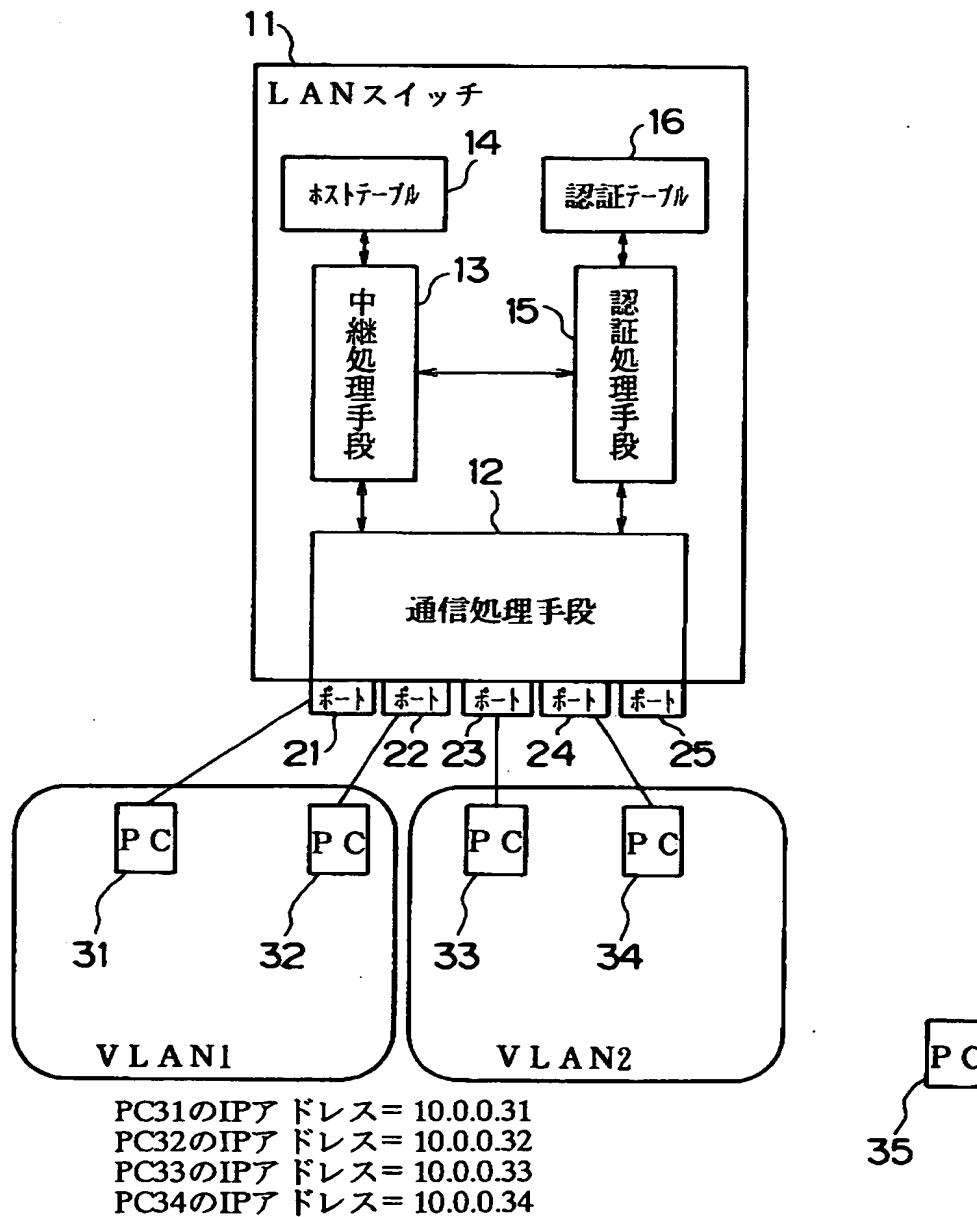
1 1 … LAN スイッチ（情報中継装置）、1 2 … 通信処理手段（制御論理）、  
1 3 … 中継処理手段（制御論理）、1 4 … ホストテーブル（制御テーブル）、1  
4 a … 始点 IP アドレス、1 4 b … 始点 MAC アドレス、1 4 c … 終点 MAC ア  
ドレス、1 4 d … ポート番号、1 4 e … 帰属ネットワーク、1 5 … 認証処理手段  
（制御論理）、1 6 … 認証テーブル、1 6 a … IP アドレス、1 6 b … ユーザ名

、16c…パスワード、16d…連絡先メールアドレス、21～25…ポート（  
入出力ポート）、31～34，35…PC、A，B，C…メッセージ。

【書類名】 図面

【図 1】

図 1



【図2】

図 2

14

14a

14b

14c

14d

14e

始点IPアドレス	始点MACアドレス	終点MACアドレス	ポート番号	VLAN
10.0.0.31	10:00:00:00:00:31	10:00:00:00:00:51	21	1
10.0.0.32	10:00:00:00:00:32	10:00:00:00:00:52	22	1
10.0.0.33	10:00:00:00:00:33	10:00:00:00:00:53	23	2
10.0.0.34	10:00:00:00:00:34	10:00:00:00:00:54	24	2

【図3】

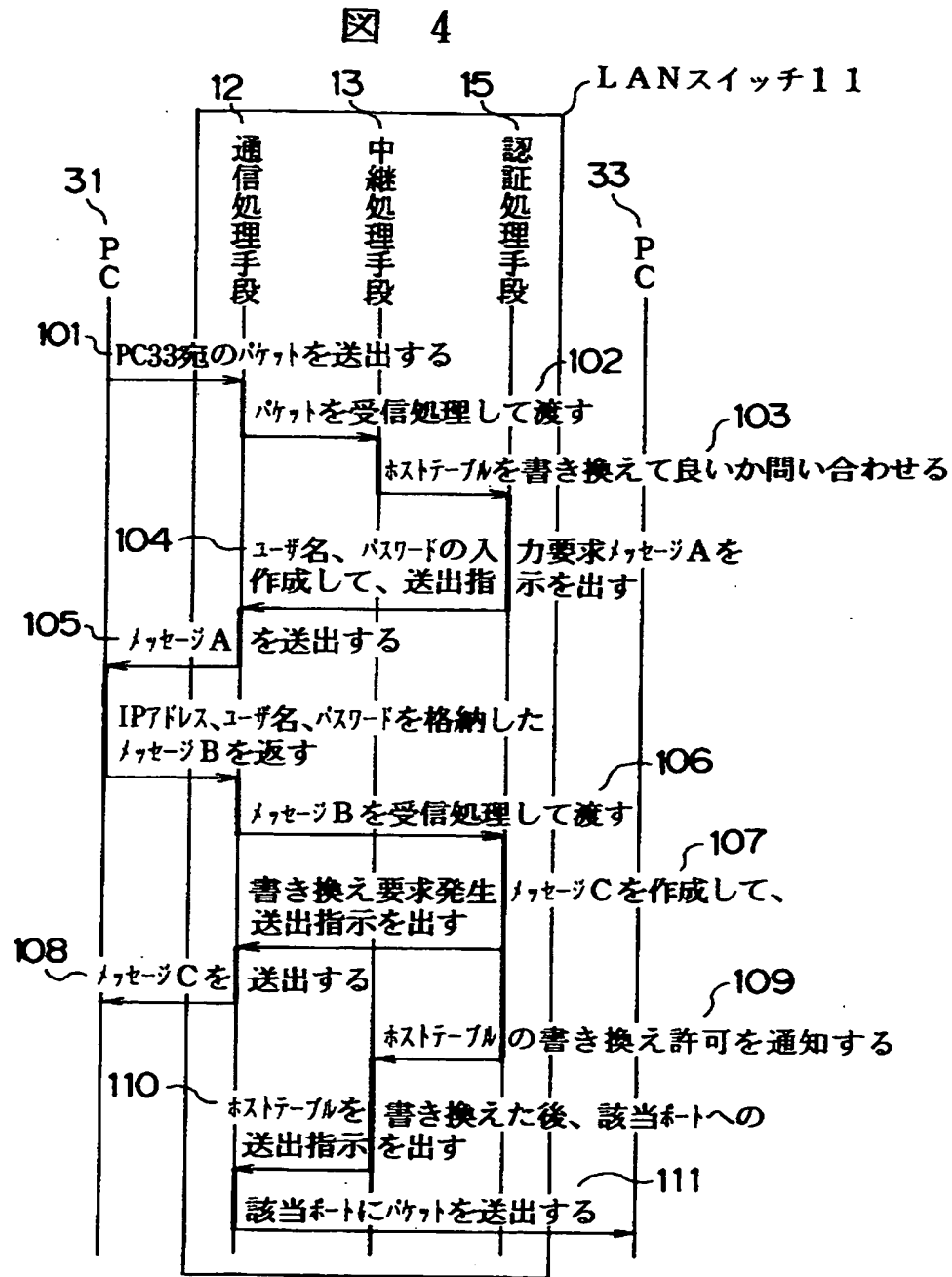
図 3

16

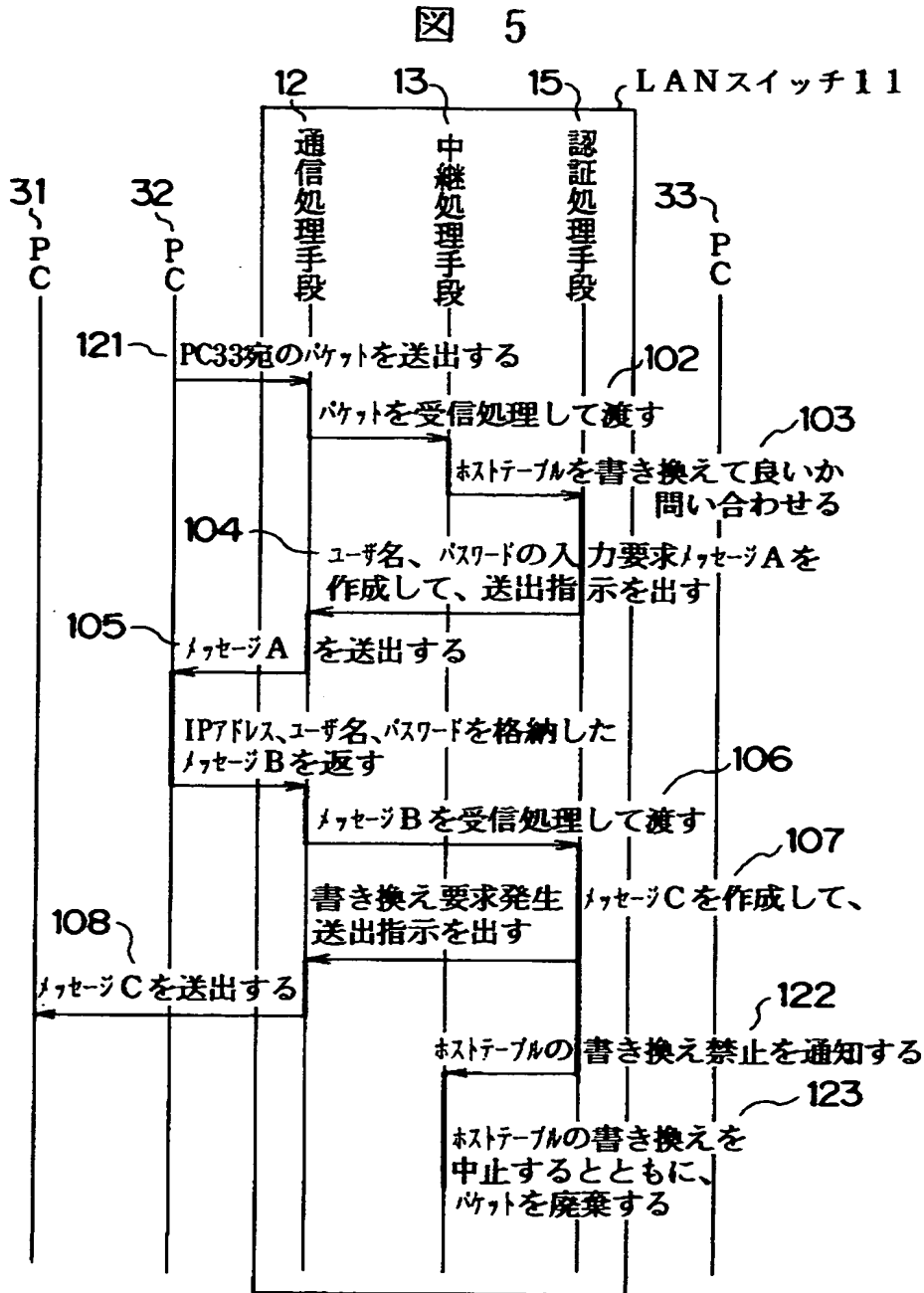
16a 認証テーブル 16b 16c 16d

IPアドレス	ユーザ名	Password	連絡先メールアドレス
10.0.0.31	PC31	pass31	pc31@hitachi.co.jp, swlla@hitachi.co.jp
10.0.0.32	PC32	pass32	pc32@hitachi.co.jp, swlla@hitachi.co.jp
10.0.0.33	PC33	pass33	pc33@hitachi.co.jp, swlla@hitachi.co.jp
10.0.0.34	PC34	pass34	pc34@hitachi.co.jp, swlla@hitachi.co.jp

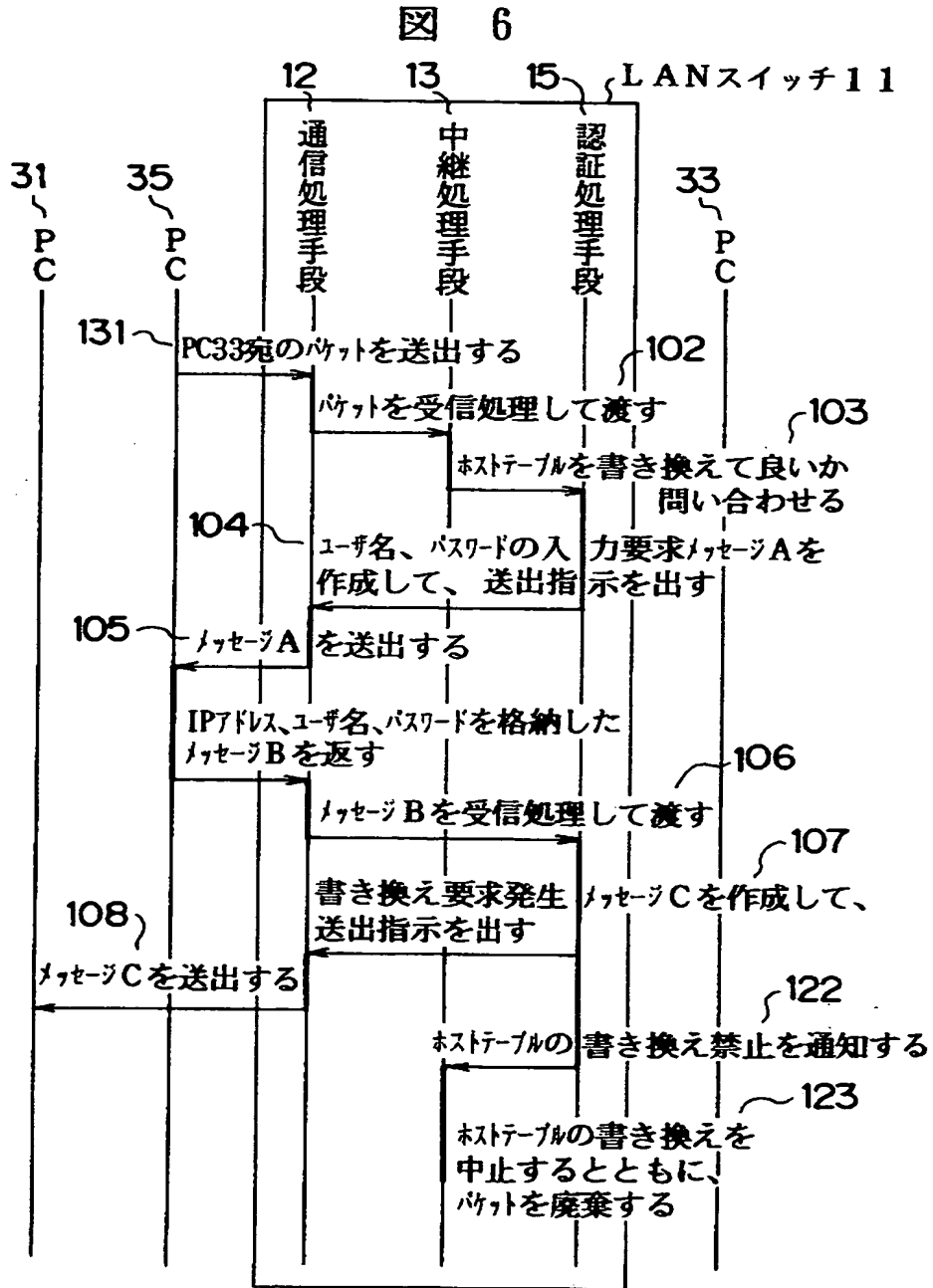
【図4】



【図5】

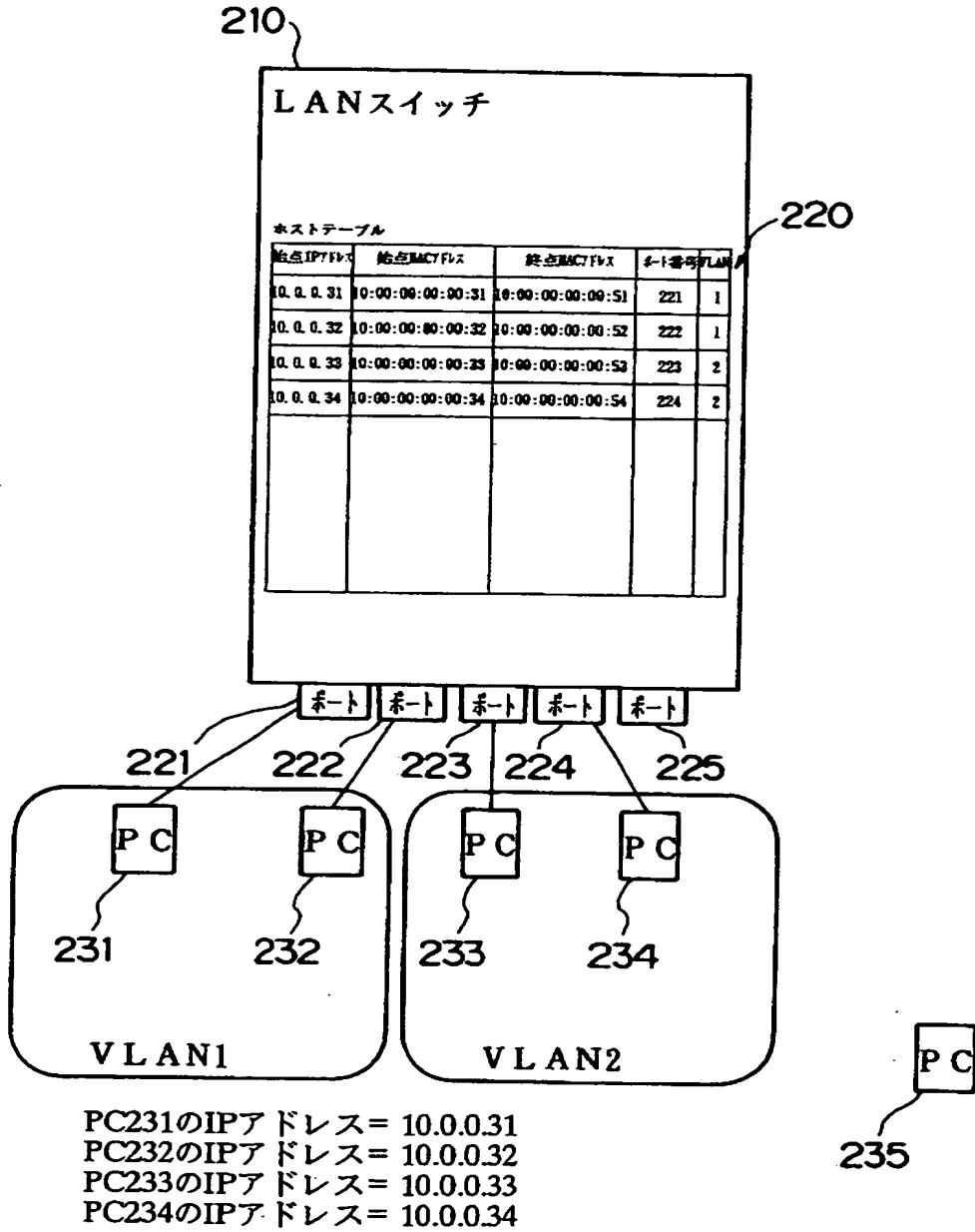


【図6】



【図7】

図 7



【書類名】 要約書

【要約】

【課題】 悪意のユーザによる盗聴やなりすましの防止、アドレス設定ミスの解析や回復を容易にする。

【解決手段】 複数のポート 21～25 の各々に任意にネットワーク端末としての複数の PC 31～34 を接続することで VLAN 1 および VLAN 2 等の通信ネットワークを構成する LAN スイッチ 11 において、各ポート 21～25 との間でパケットの送受信を行う通信処理手段 12 と、各ポートと、接続された PC のアドレス情報との対応関係の変化を学習して更新されるホストテーブル 14 に基づき各ポート 21～25 間のパケットの中継を行う中継処理手段 13 と、パケット中継契機のホストテーブル 14 の更新時に、認証テーブル 16 を参照して送信元の PC に対してユーザ認証を行い、真正のユーザの場合にのみホストテーブル 14 の書き換えおよびパケットの中継を許可する認証処理手段 15 とを備えた。

【選択図】 図 1

【書類名】 職権訂正データ  
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】  
【識別番号】 000005108  
【住所又は居所】 東京都千代田区神田駿河台四丁目6番地  
【氏名又は名称】 株式会社日立製作所  
【代理人】 申請人  
【識別番号】 100080001  
【住所又は居所】 東京都新宿区西新宿7丁目22番45号 N. S.  
E x c e l 301 筒井国際特許事務所  
【氏名又は名称】 筒井 大和

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日  
[変更理由] 新規登録  
住 所 東京都千代田区神田駿河台4丁目6番地  
氏 名 株式会社日立製作所